Analysis of Electronic Commerce Regulation in the Global Economy

Shivani Bhatia

Advisor: Dr. Deborah Ballam

The Ohio State University

For Shanti Kumari Bhatia

"Asli khushi tab milegi jab aapki likhi hui kitab mein padhoongi"

Table of Contents

I. Purpose of Writing

Being a global company is now necessary to sustain competitive advantage in many industries. However, 'going global', or doing business abroad, is not a new concept to most firms. Companies that have been doing business across borders have done so for centuries- and countries have adapted laws to support such business ever since. But there has never been a radically new medium of conducting business as the internet. In the last decade, thousands of companies starting doing business "on-line" and, because it is radically different, those who wish to adopt this new medium must have regulations, laws and rules to set guidelines, limits and define possibilities for their businesses.

Policy issues define the legal and regulatory parameters within which electronic commerce solutions are to be made available. The significance of these policy issues is the impact on the global development of electronic commerce, which is far-reaching and complex. While there is world-wide consensus that electronic commerce developments should be market-driven, specific technical and commercial developments can and do challenge the existing legal and regulatory provisions in areas such as security, taxation, financial transactions, and privacy. Given the trans-national nature of electronic commerce, a strong argument exists for a common, global approach to major policy issues. The countries have been evaluated based on the ease with which they will be able to adapt their laws if such a common global regulatory body were to be created. The levels have been evaluated based on past initiatives, the rigidity or flexibility of legislation to accommodate globalization as well as participation in the various global e-commerce initiatives that have shaped e-commerce regulation from the beginning.

II. Global e-commerce initiatives

In an attempt to encourage a global approach, several International E-Commerce Initiatives[1] have targeted different aspects of e-commerce such as digital signatures and the use of Certification Authorities to authenticate the digital signatures. These initiatives have provided the legislation bodies of the world guidelines for writing their own laws on a technology that is new, has a high impact on their businesses, and is growing very quickly. The unfamiliar and changing aspects of e-commerce have been the cause of many debates and discrepancies amongst the laws of all countries. The organizations discussed below have published guidelines and model laws that provide starting points for e-commerce legislation. Overall, the guidelines have encouraged all countries to move towards the use of similar technologies and the adoption of laws that will benefit global e-commerce. Some initiatives have been used more often than others by many countries as models for creating their own e-commerce laws. The uniformity amongst those countries has aided in the growth of e-commerce. Many such initiatives have been implemented.

The initiatives discussed below are the most widely accepted throughout the world and have been used while forming e-commerce legislation. Most of the supervisory boards of these initiatives are either a part of or supported by the United Nations.

International Chamber of Commerce (ICC)

ICC activities cover a broad spectrum, from arbitration and dispute resolution to making the case for open trade and the market economy system, business self-regulation, fighting corruption or combating commercial crime. ICC is a leader in determining standards for international usage on codes and trade definitions making it truly a global business organization. The ICC speaks for world businesses when governments take up issues such as intellectual property rights, transport policy and trade law and makes world business recommendations to the World Trade Organization. On November 6, 1997, the ICC

released its General Usage in International Digitally Ensured Commerce or GUIDEC. Addressing specifically the use of digital signatures, the GUIDEC specifies core concepts, best practices and certification issues in the context of international commercial law and practice. Specifically it is a set of common definitions and business-generated best practices for certifying and "ensuring[2]" electronic commerce. ICC allows changes and updates to achieve consensus around the terms and practices suggested in the guide and is therefore a "living document" by nature. The supervisory board is the ICC Information Security Working Party.

Internet Engineering Task Force

The IETF is a large international community of network designers, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas. An example is their current working paper in specifying the necessary data model, syntax, and processing to bind a cryptographic signature to a resource in XML, a programming language. IETF has been active in the development of global digital signatures standards since 1995.

Internet Law & Policy Forum (ILPF)

The ILPF is comprised of about 15 North American, Asian and European companies involved in technology and telecommunications. It solicits information and advice from a wide range of experts, including legal and technical experts, its member companies and other businesses, governments and intergovernmental organizations, academia, lawyers around the world.

The Forum's Digital Signature and Certificate Authorities Working Groups have conducted studies on topics ranging from the promotion of model U.S. digital signature

legislation to best practices for certificate authorities. Current goals of the Electronic Authentication Working Group include the removal of legal and tariff barriers to electronic authentication, and the harmonization of laws governing electronic authentication across jurisdictions. The regulatory bodies are Electronic Authentication, Digital Signature, and Certificate Authorities Working Groups. The ILPF is currently working with the American Bar Association and the International Chamber of Commerce on a Global Jurisdiction Survey. According to American Bar Association, "it will seek to identify when Internet jurisdiction issues emerge as serious concerns for companies operating online and which issues pose the greatest concern. With a global perspective, the survey will assess differences between jurisdictions and business sectors to gauge whether government policy concerns match the needs of corporations." This can provide a starting point for an international e-commerce regulation body.

United Nations Commission on International Trade Law (UNCITRAL)

Model International Law (Enacted)

The scope includes member states of the United Nations. It defines electronic signatures and provides for legal effect of electronic signatures, by offering a baseline for presumptions of validity.

In four Chapters, the Model Law addresses general provisions related to the definition of electronic commerce and specifies the recognition of specific qualities of digitally-produced and signed documents that can be used to establish their full legal validity. The Model law also addressed crucial factors in the communication of data messages, including contract formation, recognition by all involved parties, attribution, and receipt and acknowledgement of receipt.

Included with the Model Law (See Appendix) is a guide to its enactment, designed to provide in-depth explanations of the purposes of the Law's provisions, so that officials in Member States may better understand why specific provisions have been included and determine which, if any, of the provisions might have to be varied to take into account particular national circumstances. The model international law is essentially the basis for a framework of international e-commerce regulation.

United Nations Commission on International Trade Law (UNCITRAL): Model International Rules on Electronic Signatures

This model provides for legal effect of electronic signatures which varies depending on the level of technical reliability.

According to the drafters, the Uniform Rules are meant to provide a basic "framework" to be supplemented by technical and/or contractual regulations (determined by Member States and/or the parties to a transaction facilitated through the use of electronic signatures). For this reason, the Rules offer general provisions to establish the legal validity of electronic signatures, and specify basic rules of conduct for the parties involved in a digital signature transaction. Many countries including the United States and Singapore have adapted their laws based on the guidelines provided by the UNCITRAL. The framework is also important in providing countries newer to ecommerce with a tried method that has been adopted by the major players that would be easier to implement.

The Public-Key Infrastructure K.509 (PKIX) Working Group was established in the fall of 1995 to develop Internet standards to support an X.509-based PKI. The Working Group is now developing additional protocols that are either integral to PKI management or that are otherwise closely related to PKI use. The Group also continues to examine alternative certificate revocation methods, conventions for certificate name forms and

extension usage for certificates designed for use in (legally-binding) non-repudiation contexts, and protocols for time stamping and data certification. The relevant supervisory board is the Public Key Infrastructure (PKIX) Working Group. The X.509 technology has been accepted widely as the standard for verification of electronic documents. Because it is so wide-spread, many countries favor the technology to be the only method of determining document validity, whereas others have adopted a more open approach. These will be discussed in the next section.

III. Different approaches to electronic document validation

Overall, three approaches have emerged that determine a country's policy towards electronic document validation- Prescriptive, Minimalist and Two Tier. But before the approaches can be fully understood, several components that make the approaches different must be understood. These components are the PKI technology itself, the role of Certificate Authorities and the tendency to lean towards technologically neutral or legally specific laws.

A. PKI technology[3] Explanations

Public Key Infrastructure (PKI) is a comprehensive, generally hierarchical framework of procedures. The purpose of PKI is to enable its participants, who do not normally know each other in advance, to perform the following tasks when using open (and therefore unsecured) electronic communication networks, especially the Internet:

- mutual authentication
- confidential communication
- providing electronic documents with a legally binding digital signature

One of the essentials of a PKI is public key cryptography, which allows one key (or a small number of keys) per PKI member to be published for use by the other members so that control can be maintained over the total number of public keys that have to be managed in the system. The presence of updated cryptography legislature becomes important in evaluating the country's regulation of e-commerce in relation to the world.

A PKI also relies fundamentally on what are known as certificates, which serve as proof of authenticity for the public keys. Certificates are used mainly in connection with digital signatures. When a member receives a message containing a digital signature, the certificate first confirms that the personal data belong to the key(s) used by the sender. Secondly, it confirms that he or she is still a valid subscriber to the PKI. The validity of the signature and the authenticity of the Certificate Authorities (CA) are strictly enforced by some countries, but remain unrecognized in others. This lack of uniformity raises the question of how the Certificate Authority's liability should be allocated in the case of dispute between two parties of different countries and jurisdictions. Singapore and EU have such laws, and discrepancies so far have been handled through lengthy dialog. Therefore Certificate Authority's also become an important aspect of e-commerce regulation and their potential liability must be addressed.

B. Certificate Authorities

The EU and Singapore have addressed the potential liability of Certificate Authority's. Significantly, both jurisdictions have taken an approach that combines some variant of strict liability for certain acts or misrepresentations with a system that permits the CA to limit its liability, at least under certain circumstances. Singapore, for example, requires Certificate Authority's to specify a "recommended reliance limit" in any certificate that they issue. The recommended reliance limit then sets a cap on the Certificate Authority's

potential liability for losses caused by reliance on a misrepresentation in the certificate of any fact that the CA was required to confirm, or as a result of any failure to comply with the statutorily-prescribed requirements for issuing a certificate. Similarly, while the EU Directive generally imposes strict liability on a CA for losses caused by reliance on an inaccurate certificate or failure to abide by the requirements for issuing a qualified certificate, member states are required to permit Certificate Authority's to specify the permissible uses of a qualified certificate and the maximum value of any transaction for which it may be used. In effect, these schemes permit the CA to define the value of a particular certificate in the manner described above. [4]

C. Technological Neutrality vs. Legal Specificity

Recently, it has become increasingly important to understand the degree to which a country is technologically neutral or technologically specific when evaluating or understanding its e-commerce regulation stance. Technologically neutral in terms of e-commerce refers to countries such as the United States that adopt policies that do not state explicit technologies that are considered valid in electronic commerce contracts. As of this paper (2003) this generally means that they do not refer to Public Key Infrastructure technology explicitly in their laws, and therefore also consider valid digital signatures using other technologies as long as they meet the requirements set by that country's law.

Legally Specific countries, such as Italy have legally defined specific PKI-based laws. Most of the initiatives are "technologically neutral," although the underlying methodology clearly involves PKI technology (*e.g.*, the EU Directive, and the laws of Denmark, Spain, and Sweden). Some countries have a general law on authentication that purports to be technologically neutral, and a more specific law applying only to

communications with the government that is PKI-based (*e.g.*, Belgium, France, and Luxembourg).

These differing approaches hinder e-commerce development. Recently, the United States (neutral) and the European Union (specific) have recognized this problem and have begun negotiations to ensure that e-commerce would not be hindered because of the different approaches adopted. Although specific terms of negotiations would be too in depth in terms of this paper, it is imperative to understand that adopting a similar or same perspective might have smoothed the process and reduced the need for lengthy negotiations.

The Internet Law and Policy Forum's (ILPF) three approaches to electronic authentication legislation utilize the components discussed and explain how the world is divided on electronic commerce regulation issues.

D. Approaches to Electronic Authentication Legislation[5]

1. The Prescriptive Approach

The Prescriptive Approach's motivation often stems from a desire to establish a legal framework for the operation of PKIs - whether or not other forms of secure authentication are included or permitted - as well as a reflection of form and handwriting requirements that apply in the offline world. Legislation and regulations enacted under this approach often share the following characteristics: adoption of asymmetric cryptography as the approved means of creating a digital signature; imposition of certain operational and financial requirements on certificate authorities ("Certificate Authority's"); prescription of the duties of key holders; and definition of the circumstances under which reliance on an electronic signature is justified. This prescriptive approach allows legislatures and

regulatory agencies to play a direct role in setting standards for and influencing the direction of new technologies. Civil law countries such as Germany, Argentina and Malaysia have tended to opt for prescriptive approach.

2. The Minimalist Approach

The "Minimalist" Approach aims to facilitate the use of electronic signatures generally, rather than advocate a specific protocol or technology. The primary motivation is to remove existing legal obstacles to the recognition and enforceability of electronic signatures and records. This is ordinarily done by ensuring that electronic signatures and records fulfill existing legal requirements for tangible signatures. To the extent that there are any legislative or regulatory judgments involved in this approach, they are generally limited to defining the circumstances under which an electronic signature will fulfill any such requirements, with a goal of establishing a standard of proof. To this end, the minimalist approach focuses on verifying the intent of the signing party rather than on developing particularized forms and guidelines. Traditional common law countries such as the U.S and U.K follow this approach.

3. The Two-Tier Approach

The "Two-Tier" Approach emerged when some jurisdictions begun to realize that the first two approaches are not necessarily mutually exclusive. A "two-tier" approach represents a convergence and synthesis of the two approaches. This consolidated approach generally takes the form of enacting laws that prescribe standards for the operation of PKIs, and concomitantly take a broad view of what constitutes a valid electronic signature for legal purposes. The virtue of this approach is that it achieves legal neutrality by granting at least minimum recognition to most authentication technologies, while at the same time creating

a better-defined, more predictable legal environment by incorporating provisions for an authentication technology of choice. For example, the European Union and Singapore have directives and bills at both the minimalist level and the prescriptive level.

In order to keep the scope of this paper manageable, there is little focus on the common global approach in itself. However, given the importance of the global approach, most of the critique has been done with it in mind. Given these restrictions, the countries legislative bodies and e-commerce regulation strategies will be critiqued and highlighted for potential areas of improvement. Improvement is based on the notion that if such an approach was to become available then how easily would they be able to adopt it? The next section will discuss the organization of the analysis section.

IV. Country Specific Approaches

The next four sections will be divided by country/region- Bangladesh, the United States of America, the European Union and Singapore. These states have been chosen because together, one can understand the entire spectrum of regulations- from non-existent to overprovision. The European Union was chosen over picking an individual member state because at the level of the Union, it is easier to understand how a global approach would work if it were ever to be accomplished. The sections will include an introduction and history of their e-commerce regulation attempts (in some cases, a comprehensive list of all directives or initiatives will be made available), followed by an analysis of the current situation of the measures including identified problems or areas of improvement, and finally a recommendation section. The final section is the conclusion to this paper that will tie in the concepts discussed in this paper. The overall goals/statements that the regions have identified in entirety, the pace at which they have formulated and implemented their

initiatives, and the identified problems and strategies to overcome those problems are the basis for my analysis and recommendations.

A study prepared by the Harvard Business School titled "The Global Information Technology Report 2001-2002: Readiness for the Networked World" provided a good starting point in analyzing the progression of the countries chosen. This report ranks 75 countries on how Information and communications technologies (Its) are being used, their readiness to take advantage of ICT networks, and what opportunities and challenges remain. The report emphasizes the use of ICTs to address social and economic development goals within each country. The e-government rankings of the countries that have been evaluated are in accordance to their level of e-commerce regulation efforts. Accordingly, Bangladesh ranks the lowest (73), The United States ranks fifth, Members of the EU rank from a range of 3-26, and Singapore ranks first

A. BANGLADESH

The first country discussed is Bangladesh, which was chosen as an example of where many countries in the "global business world" stand in e-commerce regulation and infrastructure needed to support and implement the strategies/laws discussed in the introduction.

Bangladesh has no lead agency or department in charge of e-commerce regulation and policy. Bangladesh does not have many laws that relate to electronic commerce. In fact, many traditional commerce laws that could be used as foundations to pass newer laws date back to pre-independence or shortly after. With only 0.25 internet hosts per 10,000 inhabitants and 0.04 internet users per 100 inhabitants[6] Bangladesh does not yet seem to be ready for active Business-to-Consumer initiatives. However, with an increasing internet-savvy expatriate population with investing possibilities and a rapidly growing Ready-Made-Garment (RGM) industry[7], Bangladesh has a great interest in developing its e-commerce potential. Therefore, the focus of the recommendations will be on the Business-to-Business initiatives.

Although certain century-old laws are being updated, the only significant legislative changes made in recent years have not proved to be effective because of weak enforcement or provisions that allow for over-regulation (e.g. the Financial Loan Courts Act; the Securities and Exchange Commission Act). In the area of foreign trade, the legal framework is primarily governed by three legislative Acts: The Imports and Exports (Control) Act, 1950; The Customs Act, 1969; and The Foreign Exchange (Regulation) Act, 1947. Revisions and updates of these Acts are made periodically. If e-commerce regulation were to be "added" to the laws, the stipulations would fall under one of the three. The Export Policy 1997-2002 aims at promoting exports in the regional and international markets. The recently passed Intellectual Property Rights (IPR) bill of Bangladesh concentrates on software copyright protection.

1. Key legislative actions

According to the Contract Act of 1872, cross border contracts are legal. As with the Evidence Act, a physical signature is necessary to make a contract valid. However, letters by post and telegrams are acceptable in the eyes of the law. Legislation that legalizes digital certificates, electronic contracts, should also be included in their e-commerce strategy.

According to the 1881 Evidence Act (requiring physical signature on a legal contract) (The Negotiable Instrument Act, 1881; revised up to 1999), a physical signature is necessary to make any contract valid in the eyes of the law. This makes electronic contracts void under Bangladeshi law.

The 1940 Arbitration Act covers disputes arising from business transactions. Under the Act of 1940, an arbitration agreement must be in writing, though it need not be registered. The agreement might make a reference about present or future differences. Arbitration has been used customarily for the settlement of disputes between members of trade associations and between different exchanges in the securities and commodities trade. Many contracts contain a standard arbitration clause, referring to the arbitration rules of the respective organization[8].

The 1947 Foreign Exchange Regulation Act sets the criteria and conditions for holding and dealing in foreign exchange by resident entities and issues licenses to Authorized Dealers and Money Changers. It sets guidelines to monitor reporting of foreign exchange receipts against exported goods and receipt of goods against payment from Bangladesh[9].

The 1980 Foreign Private Investment (Promotion and Protection) Act provides for the promotion and protection of foreign private investment in Bangladesh. An industrial undertaking having foreign private investment shall not be unilaterally changed so as to

adversely alter the conditions under which the establishment of such undertaking was sanctioned; nor shall foreign private investment be accorded a less favorable treatment than what is accorded to similar private investment by the citizens of Bangladesh in the application of relevant rules and regulations[10].

The 1997 Intellectual Property Rights (IPR) Bill concentrates on amending the concerned laws of the British period. Bangladesh's progress in protecting the intellectual rights is at snail's pace[11]. Bangladesh has no updated law or enforcement mechanisms in Bangladesh to protect the intellectual property.

The 1998 National Telecommunications Policy ensures the orderly development of the telecommunications sector through the provision of services in all the areas of the country, to satisfy the lesser serviced demand for telecommunications and to provide equitable opportunity and competition amongst the service providers[12].

Unless Bangladesh updates its outdated laws, it will not be able to grow its electronic-commerce potential. How these laws affect its overall position in the global economy can be better assessed by looking at each of the three dimensions of e-commerce- Business to Consumer (B2C), Business to Business (B2B), and Business to Consumer (B2C).

a. Business to Consumer (B2C)

Of the three dimensions of e-commerce [13] Business-to-Consumer (B2C) e-commerce is unlikely to be of much use in the near future in Bangladesh because of low per capita income, a weak infrastructural and legal environment, and lack of trust between business and consumers. B2C for cross border trade is also limited by the factors suggested for the domestic front. In addition, difficulties in accessing international credit cards, foreign currency remittance restrictions, delays and informal payments at customs clearance even for small value and quantity items will discourage B2C. There are no laws concerning consumer protection rights, another major impediment in development of B2C.

b. Business-to-Government (B2G)

Business-to-Government (B2G) and e-government initiatives are possible in Bangladesh, but on a limited scale at this stage. The government is a major buyer of goods and services from the private sector. Typically, the government procures goods and services by inviting tenders. With e-government initiatives, the availability of the request for proposal and other relevant documents on-line provides an alternate choice to enduring lengthy paper-trail led government procedures. Transactions involving information collection, obtaining various governmental forms, and registering activities can also be conducted on-line. This will reduce time costs, corruption and the necessity of going through lengthy bureaucratic procedures that are a part of the day-to-day life at the government agencies. Another positive that could emerge as part of e-government initiatives would be an increase in transparency that would aid in eliminating corruption. No concerted effort toward e-government currently exists in Bangladesh.

c. Business-to-Business (B2B)

The Business-to-Business application already exists in the export sector of Bangladesh, especially in the Ready Made Garments (RMG) industry. The Bangladesh Garment Manufacturers and Exporters Association (BGMEA) is a powerful lobbyist organization. Any law related to e-commerce being discussed or introduced in the Bangladeshi legislative system is highly influenced and backed by the BGMEA. Given that RMG has the lion's share of the export earnings in Bangladesh, sustaining the vitality of this industry is very important for Bangladesh. Most customers for this industry are foreign companies that profit from producing their products (mostly garments) in Bangladesh, where labor costs are low. The RMG sector has begun to use the Internet, and its dependence on ecommerce is likely to grow in the coming years[14]

because the customers are technology-savvy and prefer the efficiency that e-commerce provides them in international business. The Internet would enable them to seek information about potential buyers as well as raw material suppliers and provide customers better access to order information and updates.

With the international community moving rapidly towards e-commerce business practices, Bangladeshi producers who are unable to accommodate electronic transfer of payment and other facets of e-commerce will lose the business opportunities to countries that have developed such systems. Other countries in Asia that are providers for low cost garment manufacturing are India, Pakistan, China, Indonesia, and the Philippines. All of these countries are more technologically advanced, offering similar non-distinguishable services at prices that are fairly inexpensive also. These countries will gain an advantage over Bangladeshi manufacturers in the future if Bangladesh does not update its e-commerce regulation and offer similar services.

Internet access is highly expensive in Bangladesh, with some of the highest telecommunications costs in Asia (US $ 25.46 approximately. Source: Global Competitiveness Report 2001-2002 published by Harvard's Center for International Development). With one of the lowest per capita incomes in the world, Bangladesh would benefit from the internet and e-commerce in the B2C and B2G only if it were affordable and accessible to the public.

To accomplish the above goals, the need arises for a reliable telecommunications industry. Unfortunately the Bangladesh Telegraph and Telephone Board (BTTB) continues to have restrictive pricing and regulatory strategy on ISPs despite the need for easy and affordable access to Internet services. The Bangladesh Telegraph and Telephone Board have maintained its monopoly over long distance and will be protected by NTP98 for international voice traffic until 2010. In fact, because of its control over the physical lines

in the country, the Bangladesh Telegraph and Telephone Board (BTTB) is one of the major bodies directly affecting the legal and institutional framework of Internet development in the country. Unfortunately, its monopolistic operations have more of a negative effect on the overall development of e-commerce legal framework.

The bleak picture painted so far is not the complete story. On the positive side, several policy reforms aimed at boosting the IT sector, eventually contributing to e-commerce development, have been accomplished. This includes the withdrawal of import duties from computer hardware and software in 1999. The decision to cease BTTB's role as a broker between the Internet Service Providers and the VSAT operators in early 2000 was overwhelmingly appreciated by the private sector[15] as well. Until 2000, ISPs paid an annual royalty of $3,200 to Ministry of Public Telecommunications. This was very costly for the Internet Service Providers and hindered the expansion of internet access and availability to the public. The fees charged and the earlier restrictions on the selection of VSAT carriers contributed to higher pricing for Internet consumers, thereby delaying the spread of this technology. Also, VSAT carriers are currently allowed to independently deal with the VSAT carriers. This is expected to reduce the bureaucratic delays and uncertainties that are characteristic of the ISP dealings currently. Also, Bangladesh is recognized for its pioneering efforts to take communication technologies to the poor.[16]

The government's recent decision to award an operating license for 300,000 telephones in Dhaka will meet much of the unmet demand of internet access. Discussions between BTTB and Singapore Telecom (SingTel) on laying a submarine cable between Bangladesh and Singapore have been progressing well. SingTel is expected to invest $140 million in this project. It should be kept in mind, however, that the control of this submarine cable will remain in the hands of BTTB. This means that the monopoly that BTTB enjoys will not be compromised in any way through this agreement.

Conclusions and Recommendations

The lack of legislative structure is a severe hindrance in the progress of Bangladesh's e-commerce. Bangladesh needs a regulatory body specifically created for the promotion of e-commerce to provide the private sectors and government the support and structure they need. Overall, Bangladesh rates very poorly on Harvard's study, ranking in the bottom three in all categories.

Perhaps the most significant change could be brought by bringing an end to Bangladesh Telegraph and Telephone Board's (BTTB) monopoly in the nationwide long distance services and digital data network. By doing this, private companies can aggressively start to establish small public computing sites, a characteristic of other countries such as India and the Philippines where public computing sites aided in the development of a mass of IT professionals. Also, more significantly, barriers for businesses that currently exist that include mostly dealing with the bureaucratic and expensive BTTB to become e-commerce enabled will be eliminated. Launching the Bangladesh Telecommunications Regulatory Commission (BTRC), independent of governmental control and political influence will further aid this process.

One of the easier tasks for the Bangladeshi government would be to revise the Evidence act to recognize the validity of a digital signature. Using the UNCITRALs guidelines to electronic-signatures would be efficient and relatively simple. Most importantly, it would break down one of the most crucial barriers to electronic commerce. Also, UNCITRAL has been the backbone of many countries' e-signature legislation, and therefore Bangladesh can avoid creating laws that do not follow the "international standards".

The next step would be the posting of government documents and publications including budgetary information on the Web. This positioning would help to orient government officials on the benefits of e-commerce. One approach would be offering short

courses for government officials at training centers such as the Public Administration Training Center (PATC). Bangladeshi expatriates should be sought to help with this. Political commitment to improve governance and institutional strengthening are essential for successful application of e-commerce. In other words, if the government is successful with e-commerce and the officials understand the value and potential of conducting business through technology assisted methods, e-commerce regulation in Bangladesh might become a reality in the near future.

Currently, the Intellectual Property Rights bill of Bangladesh does not address e-commerce related copyright protection. Amending this Bill to include that protection and encryption laws to accept electronic authentication of transactions would place it in line with the policies of the EU, and further its credibility in contracts.

B. THE EUROPEAN UNION

Next, the European Union's e-commerce position will be analyzed and discussed. Because many of the laws that were non-existent in Bangladesh's case are already present and regulated by the individual member states, they will not be addressed. Instead, this section analyzes the regulations and policies that the Union has undertaken as a whole.

The EU is a relatively late starter in regulating e-commerce in comparison to some countries, yet it made substantial progress in 2002 and early 2003. To date in the EU there are at least fifteen Directives[17], proposals and recommendations to try to regulate e-commerce. The impact is significant, although such regulations seem to have been introduced in a piece meal fashion. The EU has attempted to assert regulatory control of online issues and it is hoped that each country will incorporate the various EU legislative packages into local law, abolish outdated provisions, and develop an e-commerce-friendly approach throughout Europe.

In the early days of its development, the Internet was often considered a space free of rules, thereby helping the electronic marketplace to develop rapidly. In the meantime, national and international bodies like the EU, the Organization for Economic Cooperation and Development (OECD)[18] and the UN have attempted to apply traditional rules or to create new rules, that to some extent threaten the Internet's economic potential. On the 8th of December in 1999, the European Commission announced an initiative called "e-Europe - An Information Society for All" (Accenture 2001). The key objectives of e-Europe are to create a digitally literate Europe; to bring every citizen, home, school and every business online supported by an entrepreneurial culture to finance and develop new ideas; and, to ensure that the whole process is socially inclusive, builds customer loyalty and strengthens social cohesion. The commission proposed ten priority areas to achieve these objectives.

Several important differences are hindering the progression of e-Europe. First the member nations have varying opinions on the technologically neutral vs. technologically specific approach. Second, countries such as Italy and Germany favor registering of Certificate Authorities Europe-wide and requiring all foreign companies to be registered with a European licensed CA; several other members, however, oppose this approach.

The EU is in the unique position of establishing uniform policies for thirty six member states with different cultures, political views, and positions on the various factors that are important to e-commerce. In this sense, the directives and laws passed by the EU are looked upon as models for the world; indeed they serve as a test model version of the global economy. Some important directives released by the EU have been rapidly modeled by other countries even before the member states ratified them. Therefore, it is important not only for the member states of EU, but also for other countries, that a successful model be implemented. Descriptions of some of the significant directives and key legislative actions released by the EU will be discussed in the next section.

1. Key Legislative Actions (Directives)

a. Cybercrime Convention

The first international treaty on crime in cyberspace was initiated by the European Union and has been approved by the Council of Europe, Canada, Japan and South Africa. This treaty requires member countries to create laws that coincide with the regulations in the treaty regarding issues such as network attacks, digital copyrights, child pornography, computer-related fraud and viruses. The Convention was called after the "I Love You" virus fiasco of 2000 which caused losses of millions of dollars in fixing corporate IT infrastructure. The perpetrator, a Philippine citizen, could not be charged with virus distribution and hacking because the Philippines had not yet adopted cybercrime laws. The convention was the first of its kind on an international level. Although the Cybercrime

treaty was approved in May of 2001, as of March 2003 only two countries Albania and Cyprus- have actually ratified it, suggesting a weaker ratification process and inability to gain consensus from all the member states.

b. E-signature directive

The E-signature directive established a legal framework for electronic and certain certification services and organizations using digital signatures. The Electronic Signature Directive outlines the most basic requirements for signature creation devices but does not establish detailed technical industry standards or best practices. This directive, established in December 1999, require member states to legislative directive provisions by July 2001.

c. The Distance Selling Directive

This directive makes provisions, before the conclusion of the contracts, for certain information to be given to the consumer in a "clear and comprehensive manner in any way appropriate to the means of distance communication used". The way information is presented and accessible is crucial to ensure consumer protection. It is therefore important that the correct amount of information be required to be presented and, if possible, regulated so consumers are aware of disclaimer information before they proceed with the transaction. Enforcing this is easy on the internet through the use of disclaimer windows and "I accept" button prompts. The regulations currently require that a host of information be presented to the consumer prior to the purchase.

d. Data Protection Directive

This Directive had been the most discussed piece of legislation pertaining to the Internet and e-commerce since it was unresolved a few years ago. Consumers, businesses and other interest groups throughout Europe lobbied their respective parliaments to ensure that their

national interpretation was not more restrictive than the directive envisaged. Some of the main areas of concern to the DP directive were, and to some extent still are: 1) Widening the definition of processing to include everything from the collection to the destruction of personal data. 2) Attaining explicit consent prior to the processing of personal data. 3) Informing the consumer before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing. The Directive restricts the transfer of personal data to a country or territory outside the European Economic Area unless that country or territory ensured an adequate level of protection for the rights and freedoms of consumers in relation to the processing of personal data.

For many people security and privacy ranks amongst their biggest concern as it relates to e-commerce. Achieving explicit consent for the processing of personal data prior to collection has been implemented by many in the form of a check box on the web page prior to requesting the consumer to input his/her personal information. Others have used a click through button on the web page that the user has to click <OK> to prior to being asked to input personal data. Some web-sites have given consumers the option to opt-out (less have gone for the opt-in route) before personal data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing. This has been implemented with the use of a check box on the webpage. This provision arguably makes it more difficult to sell or swap mailing lists, as informing every member of any lengthy mailing list would be a huge undertaking.

The Directive provides that security and privacy of personal data has to be ensured. For businesses this means that outsourcing e-commerce projects carry with it certain legal obligations. Businesses now have to ensure that their third party employees are adequately authorized and approved by the Certificate Authority to process personal data. In fact, the Directive requires written contracts between parties to include sufficient guarantees in respect of the technical and organizational security measures that are taken to protect the

data. Due to the inherent nature of the Internet this criteria would be difficult, if not impossible, to regulate. The EU and the US held numerous high-level meetings to negotiate terms by which trans-Atlantic data transfers would not suffer.

e. E-Commerce Directive

The EU Directive on e-commerce has provisions on information requirements on the identity of service providers and on commercial communications. One of the controversial implications of this directive is the notion of with-fault liability. With-fault liability arises when an on-line intermediary intentionally or negligently violates the rights of others. The inherent nature of the internet is to give the user control over their settings. It is extremely expensive and difficult for service providers to gain complete control over their subscribers' activities on the net. Based on the country in which the issues are discussed, one activity might be illegal in Germany, but not so in France. This stipulation is only extremely difficult to execute and monitor, and thus will not be supported in the international community.

Identified Problems/Areas of Improvement

It is clear that firms in Europe are taking measures to pursue e-commerce opportunities. Three-quarters have an e-commerce strategy and more than half have developed a training plan and cost-benefit analysis. However, in the climate in which these firms operate, it is imperative that compliance with local and regional laws be a major part of that strategy as failure can be potentially costly, embarrassing and will diminish customer trust. According to successive research documents, the reasons organizations are not complying with the legislative framework are (1) unclear procedures; (2) considerable contradictory

interpretations of the regulations; (3) lack of awareness of the applicability of the regulations; (4) lack of audit, which leads to insufficient checks.

This lack of compliance may be because many of the directives have yet to take full effect in some member states. A good example is the EU Digital Signatures Directive. Discrepancies arise while determining whether the EU has taken on a minimalist or prescriptive approach. At the minimalist level, the EU Digital Signatures Directive prohibits EU Member States from denying legal effect to an electronic signature solely on the grounds that it is in electronic form, or on the grounds that it does not satisfy the standards set forth elsewhere in the directive for "advanced" electronic signatures. At the prescriptive level, the Directive affirmatively requires the Member States to give legal effect to "advanced electronic signatures" that are based on "qualified certificates" and that are created by "secure signature creation devices.[19]

Certificate Authority's role defined in the directives is crucial in understanding the future of the EU e-commerce status. Their role so far remains ambiguous because it is not clear whether digital signatures verified by Certificate Authority's credited and licensed in other countries will be acceptable.

The digital signatures directive, being a fundamental concept in e-commerce regulation, in theory should be clearly defined and understood to ensure correct interpretation by EU firms. A comprehensive, well-integrated and clearly articulated plan would play a large role in improving compliance. Therefore, developing such a plan that is accepted and implemented in a timely fashion is vital to the survival of e-Europe. [20]

Article 4(1) of the EU Data Protection Directive has been interpreted as requiring foreign website operators who automatically collect information over their websites, but who are not established for business in Europe, to comply routinely with the data privacy rules of each EU country and appoint legal representatives in those countries. This is likely to prove unworkable and unenforceable because companies not established in Europe will

find this too costly. The US was forced to go through lengthy negotiations to ensure that e-commerce would not be hindered because it did not comply with the data privacy rules of some of the countries. It will eventually become counter-productive as such negotiations might become common, thereby making it more difficult to conduct e-commerce with[21] the EU.

The one weakness of the distance selling directive is that it does not define auctions (auctions are a common e-commerce business model) and it is still unclear whether a reverse auction is subject to the Directive. Lastly, consumers are given the opportunity through the right of withdrawal, to terminate a contract within a specified period of time. The Directive defines "working days" to mean all days other than Saturdays, Sundays and public holidays. Thus, a supplier and consumer will need to take account of different public holidays in each Euro-zone member state. For consumers contracting on-line there is an issue with regards to this directive. Businesses worldwide have to consider the benefits and risks of conducting business on-line with consumers who are based in Europe because they will have to comply with all applicable laws concerning jurisdiction in each EU state.

The discussion behind the Cybercrime treaty started in 1997, and after finally being approved in 2001, the numbers do not look convincing. With the amount of cybercrime theft and corruption touching trillions, it would seem that all countries would be extremely enthusiastic about ratifying it quickly to protect their private sectors. In fact, thirty six countries (all EU countries and some others including the U.S, and Canada) have signed the treaty since November, 2001, but only two have actually ratified it- Albania and Cyprus. According to a paper written by Steven E. Billet of George Washington University, the long-term fate of the Cybercrime Convention remains in doubt, despite considerable efforts of the Justice departments of the US and the EU. He states that dual criminality concerns, the privacy, human and property rights issues will make it difficult to

be accepted by many countries- especially the U.S. These are precisely the same concerns that exist in all directives.

Conclusion and Recommendations

"The EU is a relatively late starter in adopting e-commerce but recent surveys have shown that by 2003 the EU will surpass the US in the overall value of electronic trading (Forrester Research Inc 2001). Overall, because of its cultural and ideological differences, the European Union is naturally one of the best test markets for a unified global approach. Thus, the EU is also seen as a "perfect springboard" for truly globalize trading.

Another concern that arises after researching the EU is the reaction of the corporations. Although, many European on-line businesses are aware of the EU Directives relating to e-commerce, they have not put into place plans to act in accordance with them. This may be a consequence of the huge number of Directives and the fact that many of them are yet to take full effect in all member states. Also, in the European Union member states, e-commerce has contributed to the social and economic development of the region. This is evident from the tremendous support that the EU Commission has and continues to place on the Internet and e-commerce.

Initiatives such as e-Europe prove that the technocrats and policy makers are embarking on a smooth transition from the off-line brick and mortar to on-line ventures. E-commerce is being seen as a mechanism for revitalizing the public sphere in the EU. It's geographic-less nature, common laws, and protection for consumers aids this transition.

Overall, the EU has taken great initiative to shape the international e-commerce community. The EU convention on cybercrime in November of 2001 was the first attempt to organize and brainstorm ideas to reduce the trillions of dollars that have been lost, and will continue to be lost due to cyber crimes. However, the overall theme seems to be that although EU is remarkable in initiating conversation and planning, implementation

becomes another story. Most of the problems identified for all the directives and laws revolved around ambiguity of laws and unclear procedures. With the strength and powerful leadership that the EU reflects, a clear and unambiguous standing needs to be achieved.

C. THE UNITED STATES OF AMERICA

The US is not only a leader in innovative technologies that change the world of e-commerce radically, but is also an active participant in international treaties and conventions. The US is also a firm advocate of self-regulation in e-commerce, and hence takes the minimalist approach. Australia is the only other major state that supports the minimalist approach. Discrepancies have already arisen between the US and Europe as discussed in the previous section. In an effort to provide a concise summary of the e-commerce regulations in the US, only the very influential and controversial laws will be discussed.

Compared to the other countries discusses in this paper, although it might seem strange, the United States has not been very aggressive in defining its e-commerce regulation strategy. In fact, since the e-sign act of 2000, not many major directives or initiatives have been introduced or discussed in detail—in comparison to EU and many other countries. In February 2003, the Bush administration released a document that defines the United State's government outlook towards e-commerce. The "National Strategy to Secure Cyberspace" is the first document that defines the position the government is taking, its role in regulating the internet and e-commerce, and the direction in which the government is planning on moving. Interestingly enough, this document still does not shed light on any bills being introduced or considered by the Congress that would change the current situation of e-commerce.

Key legislative actions

The Uniform Computer Information Transactions Act – UCITA – is a uniform commercial law dealing with contracts for computer (digital) information.[22] The National Conference of Commissioners on Uniform State Laws (NCCUSL) developed UCITA. The drafting

process included representatives from four Sections of the American Bar Association (ABA) and was originally suggested by the ABA. UCITA has been enacted in two states- Maryland and Virginia. Over thirty amendments were made in 2002 in response to a report of an ABA working group.

The Uniform Electronic Transactions Act or UETA creates a uniform legal framework for the use of information technology in commerce. It is designed specifically to address questions about the validity of electronic signatures, messages, contracts, evidence and record keeping as society shifts from paper-based to computer-based transactions. UETA essentially declares that electronic signatures and messages are the equivalent of their written counterparts in order to facilitate the development of e-commerce and e-government. 41 states have enacted the law so far.

Both the UCITA and UETA are important legislative initiatives that have provided the framework for an extensive state e-commerce legislation system. The US has favored state-specified rules for detailed e-commerce legislation and overall has favored industry self regulation for the setting of standards of contracts that apply specifically to companies conducting business globally. Its approach to e-commerce regulation has led to the discrepancy with the EU.

Following the UNCITRAL's guide to electronic signatures legislation, the US passed the E-sign Act in June of 2000. Under the E-Sign Act, which for the most part became effective on October 1, 2000, a signature, contract, or other record may not be denied legal validity solely because it is in electronic form, nor may a contract be denied legal validity solely because an electronic signature or electronic record was used in its formation. Electronic notarizations are also permitted. However, the Act does not require any person to agree to use or accept electronic records or signatures, except in certain cases involving government agencies.

At the end of October, 2000, President Clinton signed into law H.R. 2281, the Digital Millennium Copyright Act. The statute primarily implements two international copyright treaties negotiated through the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and WIPO Performances and Phonogram Treaty. The two treaties required the signatories to punish those who improperly circumvent technologies designed to prevent unauthorized copying of copyrighted works, such as using "black boxes" to descramble audiovideo signals, hacking into Web sites that charge for viewing, and bypassing technologies that prevent unauthorized copies of videotapes. The treaties also aimed to protect the integrity of "copyright management information," defined as information identifying the work, its author and owner, and the terms and conditions of permitted use.

Identified Problems/Areas of Improvement

UCITA was originally conceived for the laudable purpose of bringing uniformity and certainty to the rules that apply to software transactions. But critics -- including consumer groups, IT organizations, libraries, and a majority of state attorneys general -- feel the resulting draft is heavily biased in favor of large software publishers. By giving the terms of shrinkwrap and clickwrap licenses the full force of a legally binding contract, opponents say UCITA threatens a host of rights American consumers have always enjoyed. Some on the list are[23]:

- UCITA allows software publishers to change the terms of the contract after purchase.
- UCITA allows restrictions that prohibit users from criticizing or publicly commenting on software they purchased.

- UCITA allows software and information products to contain "back door" entrances, potentially making users' systems vulnerable to infiltration by unauthorized hackers.
- UCITA allows software publishers to sell their products "as is" and to disclaim liability for product shortcomings

To this extent, Americans for Fair Electronic Commerce Transactions (AFFECT), an organization created for the sole purpose to oppose the act, has formed and joined a dozen other credible organizations including the Association for Computing Machinery and American Library Associations. This act has been in debate since 1991, and as of 2003 the results still are not acceptable to major stakeholders. If consumers are convinced that the act indeed does not protect their rights, then the act will essentially contradict the overall outlook of the US on e-commerce regulation which is of self-regulation and protecting consumer rights.

The passage of E-Sign removes the key reason for states to enact the Uniform Electronic Transactions Act (UETA)—to facilitate nationwide acceptance of electronic notices and electronic signatures. UETA merely requires that the parties agree to conduct transactions by electronic means, but does not specify how that agreement is to be proven. Instead, UETA states that agreement is determined from the context and circumstances. E-Sign contains important consumer protections that are absent from UETA. Like many other federal consumer protection laws, E-Sign contemplates that states may add additional consumer protections which are consistent with the federal act. A simple electronic agreement to enter into a contract between two parties may come with a wealth of negotiations and clauses, not to mention the expense and disruption of implementing any new technology required to do so.

The Digital Millennium Copyright Act has also faced many problems. Although the treaties were signed in December 1996, widespread objections delayed ratification and

statutory implementation until October 1998. In particular, many expressed concern that the proposed implementation went further than the treaties required and unduly restricted "fair use" rights. The final version of the Act contains both exceptions and additional regulations demanded by various industry groups. Apart from implementing the treaties, the Act limits the liability of online service providers and amends the copyright laws in various other ways. This Act has represented the most comprehensive reform of United States copyright law in a generation.[24] The importance of this law lies more in the implications it has had on the laws of other legislative bodies such as the EU that has introduced its own version of the Copyright Act and is now facing much opposition by its members as well. If the Act does pass in the EU, it is possible that many countries will have to follow suit and the effects will include contradictory roles of the Internet Service Providers, which in many countries are being held responsible for the actions of its customers. The passing of such acts on a global level will lead to such discrepancies.

Conclusion and Recommendations

The US has approached the legislation process of e-commerce in a piece-meal fashion. It took twelve years to release a final version of UCITA. Ever since the final version has been available, it has faced much opposition. Because of this general sense of consumer rights remaining unprotected, the act will raise doubts and hinder its progress in being ratified in all fifty states. The other major legislative policy was the UETA, parts of which are rendered obsolete with the E-sign act of 2000. Overall, the United States has been actively involved in introducing technologies to the world, but has taken longer to pass regulations involving e-commerce. The incentive for United States e-commerce regulation originates primarily from the corporate sector rather than from government. In the long run it would be beneficial for the US to increase its regulation in order to stay current with Europe and countries it conducts e-commerce with heavily to avoid exception agreements. In addition

to this, the United States would benefit by making specific yet flexible laws that can be easily adapted to the changing environment of E-commerce.

D. SINGAPORE

Singapore began to formulate IT strategies in the 1980s, focusing on widespread computerization, expanding networks, and setting up databases. A more comprehensive nationwide approach began in 1992, as a result of the government's recognition that national competitiveness is ultimately dependent on the ability to create, possess, and apply information and knowledge. Singapore's government-driven national information technology project, *IT 2000*, was designed to make Singapore an island of information and knowledge. It has largely been implemented. The government is now creating the *ICT21 Master plan*[25] with the goal of transforming Singapore into a "vibrant and dynamic global ICT (information communications technology) capital with a thriving and prosperous net economy by the year 2010."[26] The *Singapore One* project, which developed from *IT 2000*, involved building broadband infrastructure of high-capacity networks and switches throughout the island. This infrastructure connects the government, businesses, private households and schools to an information super highway; ninety eight percent of the island's households are linked to Singapore One.

The U.S. General Services Administration found that, "Singapore's eCitizen centre is the most developed example of integrated services delivery in the world."[27] It is a single, comprehensive government web portal that brings together government services online, offering easy access to the general public. All agencies have adopted a common infrastructure and modules for form filing, payment, and security. The underlying metaphor is that of a citizen journeying through life who can stop at various "towns." Nine towns cover business, defense, education, employment, family, health, housing, law and order, and transport, and link functions of different agencies. Interestingly, the government also views eCitizen as an important public education project, because as people use and become familiar with IT their skill levels increase.

Singapore government departments have taken the lead to jump-start e-commerce activities. According to the 2002-2003 Harvard Business Student study, Singapore ranked no 1 in e-government policies and likewise in business and economic environment network policy. Several applications are already available through electronic means such as the URA Form Submission, CPF On-line and Electronic Procurement Service and Electronic Income Tax Filing.

GEBIZ is a new government initiative going online in 2003. Its goal is to create a one stop, 24-hour a day center for government business. It links the government's financial systems and procurement applications. Cost benefits are expected from more competitive bidding, quicker turn around on orders, smaller inventories and automated data collection.

The Singaporean government promotes IT initiatives in all aspects of business. For example, businesses participating in the Local Enterprise Computerization Program are given free consultations. The government also seeks to link local enterprises to multinational corporations in order to access their knowledge and technology.

Singapore has become a leader in supporting cross-certification of certification authorities (Certificate Authority's) and inter-operation of trading platforms. This supports international linkage which means linking the local infrastructure services to those overseas. In early June of 2002, the world's first international cross-certification was performed between Netrust (a Singaporean company established to manage digital keys and certificates) and a counterpart in Canada.

Singapore's participation in international discussions has been very active in ASEAN, APEC, UNICITRAL, WTO, and WIPO on e-commerce-related issues and policies. Singapore is currently the co-chair of APEC EC TaskForce and the vice-chair of the UNICITRAL Working Group on EC.

Key legislative actions/Significant Developments

The 1998 Electronic Transactions Bill treats digital signatures as a type of secure electronic signature, and establishes a comprehensive regime for their use and regulation. Singapore, like the EU, has established a two-tier approach to the verification of digital signatures, and tightly regulates the Certificate Authorities in Singapore that can authenticate digital signatures. Singapore was one of the first countries to adopt an electronic signature law after the model released by UNCITRAL.

Singapore's Electronic Transactions Bill also distinguishes between technologies based on levels of security by establishing one legal treatment for "electronic signatures," and another for "secure electronic signatures." The "electronic signatures" are generally given minimum legal effect, while the "secure electronic signatures" are entitled to an additional presumption of integrity, a presumption that the signature is that of the person with whom it is associated, and a presumption that the user affixed the signature with the intent of signing or approving the document. Singapore was one of the first countries to introduce and ratify a bill modeled on UNCITRAL.

Singapore's comprehensive cybercrime legislation appears in the Computer Misuse Act which was adopted in 1998. After the "I Love you Virus" of the Philippines, Singapore was quick to release another part to the Act to ensure legislation that would allow the government to prosecute should a similar event occur in Singapore. Part II of the Act created six new offenses: unauthorized access; access with intent to commit or facilitate commission of an offense; unauthorized modification of computer material; unauthorized use or interception of computer services; unauthorized obstruction of use of computer; and unauthorized disclosure of access code. The offences created by section 3, 4 and 5 would cover hacking, criminal intent offences and unauthorized modification of

program and data. The CMA provides that the reference to "intercept" in section 6, when used in relation to a function of a computer, includes listening to or recording a function of a computer or acquiring the substance, meaning or purport thereof. The Computer Misuse Act also criminalizes aiding and abetting and attempting to commit any of these offenses.

The legislature in Singapore has made amendments to the provisions in the Evidence Act (the "Act") relating to the admissibility of computer evidence. The amendments, effective March 1996, provide clear guidelines and rules for the enforceability of the act. The act deals with the admissibility of computer records, which might otherwise be inadmissible because computer records are usually easily alterable, often without leaving any sign of such alteration.

The E-Commerce Code for the Protection of Personal Information and communications of consumers of Internet Commerce (the "Code") was released by the National Internet Advisory Committee in September of 1998. The Code encourages providers to ensure the confidentiality of business records and personal information of users, including details of usage or transactions. It limits collection and prohibits disclosure of personal information without informing the consumer and giving them an option to stop the transfer, ensure accuracy of records and provide a right to correct or delete data.

The Code has since been adopted by CaseTrust and incorporated into its Code of Practice as part of an accreditation scheme promoting good business practices among store-based and web-based retailers. CaseTrust is a joint project operated by the Consumers Association of Singapore, CommerceNet Singapore Limited and the Retail Promotion Centre in Singapore.

Identified Problems/Areas of Improvement

Singapore might have jumped the gun by following the two-tier approach to establishing certificate authenticity. By explicitly specifying PKI technology, Singapore might encounter problems with countries such as the United States where some digital signatures might not be authorized by licensed and regulated Certificate Authorities.

The "Code" is not mandatory as it is not law. Thus Singapore has no general data protection or privacy legislation... The only substantive entity that has adopted the code so far is CaseTrust and accordingly this code of conduct strictly only needs to be complied with if one wants to seek accreditation with CaseTrust. Nevertheless, it is likely that the substance of the Code may be legislated. The NIAC came up with the Code and continues to monitor the industry adoption and implementation of this Code. It also plans to study as well as give feedback and comments on the Model Code for the Protection of Personal Information to be drawn up by the Info-communications Development Authority of Singapore (IDA). On 26 September 2000, IDA issued a consultation paper on "A Proposed Framework on Building Trust and Confidence in Electronic Commerce" inviting the public to comment on it. It is anticipated that after the close of the consultation period, the Singapore government may enact some privacy legislation in the future.[28] This is an example of the Singaporean government's efforts to quickly adapt its laws to the changing environment of e-ecommerce.

Overall, however, the government has taken an immense interest ensuring that it will be in a position to quickly alter its laws if an international law ever becomes available.

Conclusion and Recommendations

Singapore has spanned the entire range of issues associated with the legal effect of electronic signatures, the legal framework for the operation of a PKI, and the establishment of a regulatory apparatus to oversee Certificate Authority ("Certificate Authority's"). In a relatively short period of time 1997-2003, Singapore has become a leader in e-government implementations. Singapore has also acted quickly to adapt its laws to sustain the necessary regulatory framework for its five and ten year plans. It was one of the first countries to develop an electronic signature law based on the model law supported by UNCITRAL.

Conclusions

Countries such as Bangladesh are at a distinct disadvantage in international electronic commerce. Bangladesh has been struggling with outdated laws in the past few decades to get its foreign exports to the level they are at today. Now, electronic commerce has changed things all over again. Bangladesh must make another strong effort to not only update its laws but to keep those new laws "flexible" in order to accommodate international standards that will constantly change, given the nature of the technology. Bangladesh will require strong leadership, government support, and financial capital to establish the infrastructure needed to support e-commerce effectively. In order to do this, a leading committee with technical knowledge and international business experience will be essential. However, a few changes that were mentioned in the section conclusion including putting an end to the monopoly of BTTB, will give the country a boost.

The European Union and the United States are very well developed economies, leaders in technology and very active in international discussion. They have ratified the electronic signature in their laws. EU has gone further and determined that the PKI technology is the basis for which it will consider electronic contracts legal, and the US has maintained that it is technologically neutral. The discrepancies in the different positions of the two had to be resolved promptly, which turned out lengthier than assumed. Inconsistency in the overall goals of the US and EU have tangled the web of international e-commerce regulation even further. It is not difficult to envision the US and Europe becoming pioneers in crafting the basis for the cohesive global internet regulation strategy that most experts argue is inevitable. With that in mind, the EU and the US, perceived to be leaders by many other nations, must develop a coherent approach to e-commerce regulation. Taking this a step further, the EU might have to compromise a bit in its control over the Certificate Authority's and website regulation, and the US would benefit from considering some regulation of accrediting digital signatures (PKI technology).

Singapore provides a good model for countries to follow. It is transparent in its ambition to become a leader in e-commerce. To accomplish this, Singapore set achievable goals that input into its overall strategy to ensure that it will continue to be a leader. Singapore started to develop the IT infrastructure it needed decades before e-commerce gained recognition. Singapore set out, followed, and, most importantly, implemented its five-year and ten year plan accordingly. Also, Singapore continues to rapidly adjust laws that will deal with the current technology, but are not rigid to change if the industry calls for it. The EU and the US, on the other hand, are slower to introduce and ratify bills in their respective legislative bodies, and have adopted more of a wait-and-see strategy.

Michael Porter states "that the essence of strategy is choosing to perform activities differently than rivals do". [29] If the US and EU were "rivals" of Singapore in becoming the no.1 country in e-government implementation, Singapore's activities- in this case, the willingness to react to the market quicker than its rivals- will help it to sustain its competitive advantage. And, it has. In the 2001-2002 Global Competitiveness Report released by the Harvard Business School, Singapore ranked no.1 in the e-government section. Singapore is a good model for countries because it has accomplished its status through very careful planning and decisive steps. In comparison to the US and EU that have been pioneers in creating most of the technology used in e-commerce today, Singapore has caught up and then surpassed the leaders in e-commerce regulations by accomplishing the same goals with less ambiguity and in less time.

One global umbrella organization that uniformly regulates and watches the world's e-commerce is the ultimate goal, which will become increasingly difficult as the technologies and regulation increase at different paces with different perspectives. Rather than resuscitate massive legislative bodies to conform to "a standard" in the future, a standard must become widely used now. Because most countries look up to the US and EU as leaders, differences among the leaders of technology and discussion have to be resolved

before this can happen. For both the US and EU, creating uniform and unambiguous laws *now* will offset the differences that will arise with complex growth of technology later. Since Singapore strives to become the center for e-commerce, after analyzing its growth in the past two decades, it is viable to conclude that Singapore will be the first country to make changes to its regulatory system when a global standard for regulation is created. It will continue to improve itself and play a significant role in the creation of such a standard because of its involvement in the international e-commerce regulation initiatives in the past. Thus, although the US and European Union might become the leaders in the formation of a global "solution", Singapore will be the most prepared for the change when it happens.

Appendix A

Bangladesh Electronic Commerce Laws

Area	Legislation
Custom Duties	Customs Act. 1969
Import Regulations	Imports and Export (Control) Act, 1950; Customs Act, 1969; review, Appeal and Revision Order, 1977; Importers, Exporters and Indentors (Registration) Order, 1981; Licenses and Permit Fees Order, 1985
Customs Valuation	Amendments introduced to th e Customs Act, 1969, in 1997
Pre-shipment Inspection	Amendments introduced to the Customs Act, 1969, in 1998
Rules of Origin	Standard Rules of Origin, 1977
Standards	Imports and Export (Control) Act, 1950
Sanitary and Phytosanitary Measures	Imports and Export (Control) Act, 1950
Marketing and Labeling	Imports and Export (Control) Act, 1950
Anti-Dumping Measures	Amendments introduced to the Customs Act, 1969, in 1995
Countervailing Measures	Amendments introduced to the Customs Act, 1969, in 1995
Safeguard Measures	Amendments introduced to the Customs Act, 1969, in 1997
Pricing and Marketing Arrangements	Consumer Index
Export Regulations	Import and Export (Control) Act, 1950; Customs Act, 1969
Government Procurement	No legislation
Competition Law	No legislation
Intellectual Property Rights	Patents and Design Act, 1919; Copyright Ordinance, 1962; Trade Markets Act 1940
Foreign Investment	Foreign Investment (Promotion and Protection) Act, 1980
Foreign Exchange	Foreign Exchange (Regulation) Act, 1947
Banking Service	Banking Companies Act, 1991
Insurance Services	Insurance Act, 1938; Insurance Corporations Act, 1973; Insurance Rules, 1953
Telecommunications Services	Telegraph Act, 1887
Air Transport Services	Details not available from the authorities
Maritime Transport Service	Merchant Shipping Ordinance, 1993; Inland Shipping Ordinance, 1976; Bangladesh Flag Vessel (Protection) Ordinance, 1982

Source: Hossain, Najmul. "E-Commerce in Bangladesh: Status Potential and Constraints."

Appendix B

***Part One of* UNCITRAL Model Law on Electronic Signatures with Guide to Enactment. (2001)**

Article 1. Sphere of application
This Law applies where electronic signatures are used in the context*of commercial** activities. It does not override any rule of law intended for the protection of consumers.
Article 2. Definitions
For the purposes of this Law:
(a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message;
(b) "Certificate" means a data message or other record confirming the link between a signatory and signature creation data;
(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy; and acts either on its own behalf or on behalf of the person it represents;
(d) "Signatory" means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents;
(e) "Certification service provider" means a person that issues certificates and may provide other services related to electronic signatures;
(f) "Relying party" means a person that may act on the basis of a certificate or an electronic signature.
Article 3. Equal treatment of signature technologies
Nothing in this Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law.
Article 4. Interpretation
1. In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.
2. Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.
Article 5. Variation by agreement
The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.
Article 6. Compliance with a requirement for a signature
1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and
(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
4. Paragraph 3 does not limit the ability of any person:
(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or
(b) To adduce evidence of the non-reliability of an electronic signature.
5. The provisions of this article do not apply to the following: [...].

Article 7. Satisfaction of article 6

1. *[Any person, organ or authority, whether public or private, specified by the enacting State as competent]* may determine which electronic signatures satisfy the provisions of article 6 of this Law.
2. Any determination made under paragraph 1 shall be consistent with recognized international standards.
3. Nothing in this article affects the operation of the rules of private international law.

Article 8. Conduct of the signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:
(a) Exercise reasonable care to avoid unauthorized use of its signature creation data;
(b) Without undue delay, utilize means made available by the certification service provider pursuant to article 9 of this Law, or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if:
(i) The signatory knows that the signature creation data have been compromised; or
(ii) The circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised;
(c) Where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.
2. A signatory shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 9. Conduct of the certification service provider

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:
(a) Act in accordance with representations made by it with respect to its policies and practices;
(b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;
(c) Provide reasonably accessible means that enable a relying party to ascertain from the certificate:
(i) The identity of the certification service provider;
(ii) That the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued;

(iii) That signature creation data were valid at or before the time when the certificate was issued;
(d) Provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise:
(i) The method used to identify the signatory;
(ii) Any limitation on the purpose or value for which the signature creation data or the certificate may be used;
(iii) That the signature creation data are valid and have not been compromised;
(iv) Any limitation on the scope or extent of liability stipulated by the certification service provider;
(v) Whether means exist for the signatory to give notice pursuant to article 8, paragraph 1 *(b)*, of this Law;
(vi) Whether a timely revocation service is offered;
(e) Where services under subparagraph *(d)* (v) are offered, provide a means for a signatory to give notice pursuant to article 8, paragraph 1 *(b)*, of this Law and, where services under subparagraph *(d)* (vi) are offered, ensure the availability of a timely revocation service;
(f) Utilize trustworthy systems, procedures and human resources in performing its services.
2. A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of paragraph 1.

Article 10. Trustworthiness

For the purposes of article 9, paragraph 1 *(f)*, of this Law in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are trustworthy, regard may be had to the following factors:
(a) Financial and human resources, including existence of assets;
(b) Quality of hardware and software systems;
(c) Procedures for processing of certificates and applications for certificates and retention of records;
(d) Availability of information to signatories identified in certificates and to potential relying parties;
(e) Regularity and extent of audit by an independent body;
(f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or
(g) Any other relevant factor.

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure:
(a) To take reasonable steps to verify the reliability of an electronic signature; or
(b) Where an electronic signature is supported by a certificate, to take reasonable steps:
(i) To verify the validity, suspension or revocation of the certificate; and
(ii) To observe any limitation with respect to the certificate.

Article 12. Recognition of foreign certificates and electronic signatures

1. In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:
(a) To the geographic location where the certificate is issued or the electronic signature created or used; or
(b) To the geographic location of the place of business of the issuer or signatory.
2. A certificate issued outside *[the enacting State]* shall have the same legal effect in *[the enacting State]* as a certificate issued in *[the enacting State]* if it offers a substantially equivalent level of reliability.
3. An electronic signature created or used outside *[the enacting*

State] shall have the same legal effect in *[the enacting State]* as an electronic signature created or used in *[the enacting State]* if it offers a substantially equivalent level of reliability.

4. In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.

5. Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.[30]

Part IV of General Usage in International Digitally Ensured Commerce

1. General

Although many of the technological issues pertaining to global digital commerce are being readily addressed, significant legal questions remain unresolved, posing significant barriers to further development of a global electronic trading system. The continued vitality of the emerging global electronic trading system depends on the progressive adaptation of international and domestic laws to the rapidly evolving networked infrastructure. Although analogy to existing rules may be possible in many cases, the application of pre-existing rules that have not been reconsidered in light of progressive technologies may lead to inappropriate results. Applying paper-based rules to electronic transactions without sufficient consideration of the ramifications of such rules increases uncertainty, working to the detriment of the international trading community.

Similarly, conflicting legislative efforts directed at facilitating electronic commerce at the domestic level can effectively deter the development of a coherent global framework. This concern applies both to consistency among individual domestic states and consistency between nations, amplifying the need for convergence and harmonization in legislative approaches. Substantive and procedural legal incompatibilities between countries threaten to create a complex and unpredictable environment for international electronic commerce.

The increasing importance of open networks such as the Internet, which promotes borderless interactivity between users, compounds the need for a uniform and harmonized approach to developing an international legal infrastructure for ensuring. The increasing importance of raising the level of trust and reliability in these new communications systems stimulates the need for a globally coherent, unified regulatory approach to information security, and in particular ensuring and certifying messages.

2. Form Requirements

The traditional rationale for requiring the formalities of a signed writing for commercial transactions has been to discourage reliance on oral agreements. The requirement of a written record of commercial transactions has also endured for regulatory purposes, such as to discharge administrative tariffs and fees associated with taxation, customs, et cetera. Despite this traditional formality, however, writings have not been required to the exclusion of other evidence of a transaction or agreement. Indeed, in common law countries, where requirements for writing may exist in the context of sales of goods, writing is loosely defined as anything that contains the essential elements of the contract. Under civil law regimes, writing is merely treated as better evidence than the lack of one.

Nevertheless, the use of digital signatures for commercial purposes faces a number of existing legal impediments that derive from both common and civil law treatment of form requirements for many types of commercial transactions. In both the common and civil law traditions, existing law imposes specific requirements relating to written, signed, certified, and/or original form which do not contemplate the use of electronic messages. Several areas of the law, such as land law, are rife with requirements relating to form that

presuppose the use of a traditional pen and ink signature on a paper message. This is especially true in the civil law, where form requirements for transactions involving not Arial, Helvetica, sans-serif intervention impose a rigidly defined legal regime for authenticating commercial and other messages.

3. Common Law Issues

One of the most nettlesome problems arising out of the use of electronic means of communications in common law-based jurisdictions derives from uncertainty as to whether or not electronic transmissions satisfy the writing and signature requirements to be found in the Statute of Frauds, embodied in United States law in U.C.C. Article 2-201, or originally in section 40 of the English Law of Property Act 1925, now to be found in section 2 of the Law of Property (Miscellaneous Provisions) Act 1989. Because there is virtually no case law regarding these issues involving the use of electronic means for transacting commercially, general thinking on the question of electronic messages as signed writings has focused on common law commercial theory and judicial precedent involving other forms of non-traditional writing used in commerce, such as teletype and facsimile evidence.

The U.C.C. defines "signature" as "any symbol executed or adopted by a party with present intention to authenticate writing." The Official Comment to section 1-201 emphasizes that the appropriate focus of the signature requirement is the "intention to authenticate" rather than the manner of symbol adopted by the parties. This is borne out by the courts, which have found a number of non-written signatures to be the functional equivalent of one, including a typewritten name, a hand printed name, company letterhead, a sales brochure, and a tape recording. Although these interpretations would suggest that ensuring techniques probably satisfy statute of fraud requirements for signatures, this is unclear without specific judicial precedent or statutory provision.

4. Civil Law Issues:

Civil law systems typically contain a variety of form requirements. For example, under German Law, contracts may generally be concluded if the parties have given declarations of will to be bound. As a general principle, such a declaration may be given electronically, such as by ensuring the message.

However, there are many cases where statute or the relevant code of laws require that certain declarations of will be made in written form; in such cases, the code defines what it means - generally a written signature made by pen on paper. This is the case in German and French law with respect to real estate, and contracts which do not observe this written form are considered to be void.

5. Consequences

The historical and currently perceived function of formalities has an important effect on their adaptability to electronic commerce. The advent of electronic commerce has challenged, and will continue to challenge, the validity of these formalities. As electronic commerce becomes more and more a reality in the international trade, the function of legal formalities which govern these transactions must evolve to include electronic means. At the present time a number of national and international efforts to treat the use of digital messages, including message ensuring techniques, have begun to address form

requirements as a legal barrier to electronic commerce. Many of these efforts, particularly those state-based legislative implementations in the United States treating the use of digital signatures, as well as related efforts in Australia, Austria, Chile, Denmark, France, Germany, Italy, Japan, Malaysia, Singapore, South Korea, Sweden, and the United Kingdom, have been influential in the drafting of this document.

The United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, certainly the most comprehensive international legal treatment of form requirements as they relate to electronic commercial transactions in existence today, is also extensively drawn upon in the GUIDEC.

Appendix D

List of Acronyms

B2B	Business to Business
B2C	Business to Consumers
B2G	Business to Government
BGMEA	Bangladesh Garment Manufacturers and Exporters Association
BTTB	Bangladesh Telegraph and Telephone Board
CA	Certificate Authority
EU	European Union
ISP	Internet Service Provider
OECD	Public Administration Training Center
PKI	Public Key Infrastructure
RGM	Ready-made garment industry
UCITA	Uniform Computer Information Transactions Act
UETA	Uniform Electronic Transactions Act
UNCITRAL	United Nations Commission on International Trade Law
VSAT	Very small Aperture Turnover

References

Accenture 2001, "E-Europe: Connecting the dots?" 17 August, 2002. <http://www.accenture.com>

Baker, Stewart, Rosa Barcelo, Eric Greenwald and Chris Kuner. "An Analysis of International Electronic and Digital Signature Implementation Initiative." 2000.

Billet, Steven E. "Transnational advocacy and the cybercrime convention: A consideration of lobbying and global governance." American Political Science Association Annual meeting presentation (2002).

Blanning, Robert We. Tung X. Bui and Margaret Tan. "National information infrastructure in Pacific Asia." Decision Support Systems. (1997): 215-227.

Church, David, Pullen, Mike and Jane K. Winn. "Recent Developments Regarding U.S. and EU Regulation of electronic Commerce." The International Lawyer. American Bar Association, 1999

Convention of Cybercrime Page. Council of Europe. 6 March 2003 <http://conventions.coe.int/Treaty>

Cyber-Crime Page. Privacy International. 27 March 2003 <http://www.privacyinternational.org/issues/cybercrime>

Diedrich, F (October 2000); "A Law of the Internet? Attempts to Regulate Electronic Commerce"; JILT (Journal of Information, Law and Technology). 17 October 2002. <http://elj.warwick.ac.uk/jilt/00-3/diedrich.html>

E-Commerce Page. Singapore. 27 March 2003. <http://www.ec.gov.sg/singapore/timeline/ecmasterplan.html>

Electronic Commerce Projects Ad hc Task Force. Jurisdiction and Applicable Law in Electronic Commerce. 15 April 2003 <http://www.iccwbo.org/home/statements_rules/statements/2001/jurisdiction_and_applicable...>

"E-commerce and the consumers interest - legal aspects of e-commerce and the consequences for SME's", Bureau European de Unions de Consommateurs (BEUC) -BEUC/064/99.

Endeshaw, Assafa. "Regulating E-commerce in Indonesia" Lessons from Asian and Beyond." Computer Law and Security Report. vol 18 (2002):352-355.

E-Ping Page. European Parliamentarians Internet Group. 5 March 2003 <http://www.eping.org/members.html>

EU Forum on Cybercrime.2001.Brussels, Belgium, (6 November 2001). Retention of Traffic Data.

Jahankhani, Hamid; "The impact of law on e-business practices in EU", University of East London.

Harvitz, Robert. "Regulatory Framework for E-commerce: International Best Practices and Models." Global Internet Policy Initiative. 2002

Henderson, Keith. "Cybercrime and Corruption." osOpinion. (2000). 5 March 2003 <http://www.newsfactor.com/perl/story/6056.html/>

Hossain, Najmul: E-commerce in Bangladesh: Status, Potential and Constraints, December 2000, University of Maryland, College Park.

Kuner, Christopher. "Beyond Safe Harbor: European Data Protection Law and Electronic Commerce." American Bar Association, 2001.

McCallum. Aspects of Doing Business in the United States. Warner Narcross and Judd LLP, 1999.

Paulson, Greg. "Cybercrime Treaty." The Sans Institute. 27 March 2003 <http://www.sans.org/rr/legal /treaty.php>

Sax, Michael M. International Law Issues Relating to Electronic Commerce. 1999.

The Council of Europe Cybercrime convention. "A civil liberties perspective." The COE Cybercrime Treaty. March 2003. <http://www.efa.org/au/publish/coc-paper.html>

Verton, Dan. "Cyberthreats Not to Be Dismissed, Warns Clarkw." Computer World. 5 March 2003. <http://www.computerworld.com>

Wall, Bill. "An imperfect Cybercrime Treaty." CIO Magazine. (2002).

Wang, Kien Keang and Ken Chia, "Singapore." E-com Legal Guide. Jan. 2001

Wegenek, Robet., O'Neill., Ged, and Moore, Jonathon. E-commerce : a guide to the law of electronic business. London: Buttersworth, 2002.

[1] Source: An Analysis of International Electronic and Digital Signature Implementation Initiatives: A Study Prepared for the Internet Law & Policy Forum (ILPF) September, 2000

[2] An example of this global perspective is the term: "ensure". In American usage, the term "authenticate" is the term used to describe how a person uses a digital seal or signature to identify with a message. In many other countries the term "authenticate" has a different and established meaning - it is how third party officials (such as Notaries / Notaires) identify parties to a message or document. Rather than create an ambiguity in terms of practice and definition between paper and electronic methods, the drafters of the GUIDEC sought to introduce the use of a term with no contrary established legal precedent. The plain English meaning of "ensure": *to make secure or certain; make safe, as from harm* embodies this aim perfectly, thereby giving it a pivotal place within the GUIDEC.

[3] www.gdm.de 2002 by Giesecke & Devrient GmbH, Prinzregentenstr

[4] Internet Law and Policy Forum, Survey of International Electronic and Digital Signature Initiatives

[5] Minutes of the fifth meaning of the ITLF. www.tremu.gov.pk

[6] Harvard Business Country Profiles. Bangladesh receives bottom of the barrel ratings in Networked Readiness related factors (Overall 73 out of 75).

[7] Ready made garment industry

[8] Bangladesh Bank. 19 May 19, 2003 <http://www.bangladesh-bank.org/about/dept/fepd.html>

[9] ARBITRATION LAW IN BANGLADESH. 03 May 2003. <http://www.vakilno1.com/saarclaw/bangladesh/arbitrationlaw/arbitration_law_in_bangladesh.htm>

[10] FOREIGN PRIVATE INVESTMENT (PROMOTION & PROTECTION) ACT, 1980 13 April, 2003. <http://www.bdmail.net/bepza/for_inv.htm>

[11] "HC declares SSA's project illegal". The Daily Star. 01 December, 2002

[12] National Telecommunication Policy of Bangladesh. 29 January, 2003. <http://www.bttb.net>

[13] Business-to-Consumers (B2C), Business-to-Business (B2B) and Business-to-Government (B2G)

[14] Hossain, Najmul E-Commerce in Bangladesh: Status Potential and Constraints.

[15] E-Commerce in Bangladesh: Potential and Policy Priorites. Recommendations arising from brainstorming session.

[16] GrameernPhone is the best-known example, with its venture to introduce cellular payphones in villages.

[17] The legal regime in the EU and their impact on e-commerce business practices Directives are the most common forms of European legislation. They are essentially instructions to the Member States to introduce laws in their own parliament. In general they indicate the goals to be achieved not the manner of achieving them. Inmost cases it is left to the national parliaments to interpret the Directives and bring about the necessary mechanism for implementing them in their own countries. On average, Member States have a two-year transition period to translate a Directive in to national law. There are also other initiatives such as proposals and recommendations, which are a little more relaxed in nature

[18] Organization for Economic Cooperation and Development (OECD). 09 March, 2003. <www.oecd.org>

[19] Accenture 2001, "E-Europe: Connecting the dots?" Cited August 2001, http://www.accenture.com

[20] The impact of law on e-business practices in EU, Hamid, Jahankhani, University of East London, According to Jahankhani, although EU has substantially improved in terms of directions, their progress in implementation continues to be slow particularly because of the number of directives issued, and the fact that many members have yet to enact the majority of them.

[21] Saleem, Omar Copyright (c) 2000 The John Marshall Law School, The John Marshall Journal of Computer & Information Law, Fall, 2000 "THE ESTABLISHMENT OF A U.S. FEDERAL DATA PROTECTION AGENCY TO DEFINE AND REGULATE INTERNET PRIVACY AND ITS IMPACT ON U.S.-CHINA RELATIONS: MARCO POLO WHERE ARE YOU?"

The EU Directive places considerable pressure on the U.S. to regulate Internet privacy and provide adequate protections. The EU Directive's requirement of adequate protection and government regulation caused grave concerns for U.S. businesses with a preference for self regulation. Although the U.S. did not join as one of the member states that adopted the EU Directive, the U.S. later reached a safe harbor agreement with the EU. This agreement was reached through the U.S. Department of Commerce to encourage the implementation of effective protections for consumer privacy on the Internet. The approach taken in the safe harbor agreement is

a departure from the EU Directive. While the EU Directive seeks to promote the creation of privacy laws by member states, the safe harbor agreement seeks to encourage self-regulatory efforts in the private sector for data collection and dissemination. Under the safe harbor Agreement, a U.S. company must register with the FTC, commit itself to comply with the EU Directive, notify customers when data is collected, provide for an opt-out opportunity, and allow Internet users to obtain and modify information held by the company. Adherence to the principles of the safe harbor Agreement is entirely voluntary.

The cultural and jurisprudential differences between the EU and the U.S. are depicted in their different policies and practices to governing Internet privacy. Privacy protections under the EU Directive are stricter than in the U.S. Under the EU Directive, privacy is a fundamental right, whereas, in the U.S., privacy has developed more piecemeal and state-by-state. In the U.S., for example, most state legislatures discussed, debated or passed privacy legislation during their respective 2000 legislative sessions. In addition, the U.S. Supreme Court, unlike the EU, has not recognized a fundamental right to privacy. Rather, the Court has addressed various issues related to privacy and found privacy rights implicit in the Bill of Rights.

Furthermore, unlike the EU, data privacy in the U.S. has been construed as a matter of commerce rather than a fundamental right because the power to regulate Internet privacy is within the jurisdiction of the FTC. In a report to Congress, the FTC suggested legislation to establish standards for the collection and use of information online for profiling and the creation of an agency to enforce those standards. The FTC also emphasized that self regulation by the private sector was the most effective and least intrusive method to ensure fair trade, access, choice, security, enforcement and other consumer protections on the Internet. Despite the different approaches adopted by the U.S. and the EU to regulating Internet privacy, both have begun serious consideration of the issue. Notwithstanding these efforts, the global nature of the Internet makes its regulation a matter beyond the geographical boundaries of the U.S. and Europe.

[22] UCITA.org

[23] Computer Professionals for Social Responsibility http://www.cpsr.org/program/UCITA/ucita-fact.html

[24] educause www.educause.edu/issues/dmca.html

[25] Masterplan explanation

[26] E-Commerce Page. Singapore. 27 March 2003 <http://www.ec.gov.sg/singapore/timeline/ecmasterplan.html>

[27] The United States General

[28] E-com legal guide to Singapore

[29] What is Strategy? (Page 64) Harvard Business Review, November-December 1996

[30] UNCITRAL home page. 28 March 2003. <www.uncitral.org>